

## **WNYRIC IT Leaders Brief: Tablet and Smartphone Integration Strategies 2011**

**April 20, 2011**

### **Introduction:**

The conversations regarding the safety and effectiveness of allowing smartphones and tablets into our schools has been active this year, not only in K-12 settings, but also in business. We can observe the business models thus far and with the help of Gartner and InfoTech as well as other sources state plainly that attempts by businesses to ban, discourage and control the use of these devices have been unenforceable. The more the IT Departments push the organization standards the more employees will go outside to find the tools they want which opens up security holes.

### **Issues for Consideration:**

**Businesses** do not need tablets and smartphones to function for increased productivity – a laptop and a phone are still good enough to use. This market is exploding because the end user is dictating what they want, and IT Departments are not. There is no documented business argument for integrating tablets into your environment – they are useful, but you can do all your work with current tools.

In **the K-12 arena** we have an Erate pilot report conducted by Watkins Glen and GST BOCES which clearly indicates that utilizing smartphones (mobile learning devices) increased student achievement in NYS assessments in ELA and Math. The classroom teachers in the pilot stated that there were significant gains in mastery- level achievement largely attributed to the dramatic increase in the amount of time students were on task and digital access to course content and online applications. There is more information in the full document which is available upon request.

In **the vendor market** there is a war (ARM processors – that have OS that are different than Microsoft) and the products revolve around the **browser** and now companies like HP are moving their OS on PCs to this browser base and there is now a battle in the PC market. The concerns with standardization and enterprise management we are having today with tablets and smartphones will bleed into the Netbook and laptop market as vendors move to “browser operating systems”.

**Hardware Development** -There isn't a lot of innovation in the ergonomics of the devices – form factors have stabilized (clamshell, convertible, open-face, hybrids [wearables]) so the efforts are being made in application development. This is different for the marketplace than previously seen.

**Application Development** – An example of new application strategies include those being developed in 2011 which have the smartphones and tablets being used in the business environment for mobile payments. This is just going to get bigger and our currency is changing. Mobile devices (with web services) have now been integrated into common electronic equipment (clock radio with iPad adaptor), car starters, etc. Web site development has changed to XML readability as it must be accessible from mobile devices as this is going to be one of the primary access tools.

## **Management of Resources:**

**The Measurement of Great Tablets** (criteria) – Currently the Motorola Xoom and the iPad2 have been rated A+ in the tablet arena because they meet the following criteria (iPad also has great marketing):

- Dual core processors
- Wifi version of the device costs less than \$500.00
- Instant on feature
- Self contained - 16 x 9 tablet screens with thinner bezel (7 inch is too small and not 16 X10- too big)
- Intuitive user interface
- Video camera integrated
- > 30,000 applications are available.

**Enterprise Management Concerns in the market currently** - these devices predominately surround the web based services utilized:

- Security – where is our information and who has access
- Single Point of Failure to the web
- K-12 – content filtering to align to CIPA
- Enterprise Management limitations based on the OS (current):
  - The Android tablet and Smartphone– the application downloaded can only see its BIOs section of the OS so it is impossible for a single application to monitor the entire environment. The user has to be involved.
  - Apple – IOS devices - third party management server allows access – there is a certificate put in the device and then whenever there is an app downloaded the app is given a key on the device so there is no split. To remove device – then remove the certificate and all applications go away (this is new).

All updates through iTunes (at home or at work?) – The user is still involved in the process and considering the history of the laptop – this still creates support calls. This makes sense for the consumer side – not the enterprise side.

## **Enterprise Management Concerns in the market future –**

- Network Access – the devices need to re-authenticate in less than 100 ms to allow video and telephony.
- Authentication systems will blend roaming and security in a single model – but we are not there yet.
- Encryption is only available on the iPad2 and will be available on Android 3.1 (Ice Cream – not on Honeycomb).

**Foundation of Context and Collaboration** –these devices are so very different and the use is changing the way we work:

- The **user** controls who they want to collaborate with and the system figures out the best way for the user to do that. The system also decides the context as to how you receive the information. Rather than the user going to get them (Google search is no longer applicable) – example - as you enter a store, the coupons are sent to your device.
- Mobile collaboration client – multiple data sources in a single view with multiple layers, so not a single URL.

### **Conclusion:**

These devices are changing how we enforce Standards -

- Security, patch management, governance, risk and compliance, inventory – the IT Department will not have the authority over the device. Must have the following:

Acceptable Use Policies – can include the following language as an example -(Policy Services can help) **This policy is intended to establish general guidelines for the acceptable student use of the DCS and also to give students and parents/guardians notice that student use of the DCS will provide student access to external computer networks not controlled by the School District. The District cannot screen or review all of the available content or materials on these external computer networks. Thus some of the available content or materials on these external networks may be deemed unsuitable for student use or access by parents/guardians.**

**Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events. Parents and guardians must be willing to establish boundaries and standards for the appropriate and acceptable use of technology and communicate these boundaries and standards to their children. The appropriate/acceptable use standards outlined in this policy apply to student use of technology via the DCS or any other electronic media or communications, including by means of a student's own personal technology or electronic device on school grounds or at school events.**

- Verify insurance, audit compliance and legal compliance.
- Access and roaming control – as users get onto different networks the system has to ensure that they have to correct system – this is coming, but not ready yet.
- A device has to be capable of being cleaned of all content "over the air" (OTA), should the device be reported as lost or stolen (removal of the certificate and keys) – available on iPad2
- Force the user to employ a complex password consisting of a combination of uppercase and lowercase letters, numbers and special characters, with the ability for periodic changes.

- Encryption is now a suggested option for appliance-level devices. This is suggested even when it causes some user inconvenience, slight performance degradation or has not been proven in all tested security scenarios. Encryption will remain a suggested option until YE11, at which time, Gartner believes, most mainstream endpoint operating systems with at least 10% share of their respective market will have robust solutions. At that time, we expect vendors will make encryption mandatory.
- Governance and Risk – Must have the following - Acceptable Use Policies, ensure auditors find this utilization as acceptable, insurance compliance; legal compliance should be in place. Xoom and iPad 2 – both have encryption – Honeycomb (post android 2.3) is launched to go encryption **after** the tablet market.
- Organizations that permit individually liable devices to connect to enterprise e-mail systems under the appliance level must require the user to sign documents that enforce at least three policies:
  1. As a condition of employment, the end user must report any lost or stolen device to IT immediately upon detection.
  2. When reported lost or stolen, the user grants permission for the device to be wiped of its contents. This policy is necessary to ensure that an end user who has invested in personal music, but who hasn't backed it up, doesn't make a compensatory claim for reimbursement.
  3. And, lastly, to prevent misuse, users must be told that these devices are for their own convenience, but that all e-mail and attachments must be read on standard PCs and notebooks. This prevents the user from believing that a mobile or other non-PC endpoint device is a notebook substitute and blaming IT for any document conversion mistakes inherent in non-Windows platforms.

**WNYRIC Support** -iPad and Samsung Galaxy Tablets will be listed as approved devices through CSLO with approval of Michelle Okal. CSLO is only approving these devices with wifi only and for use in the district and may not be taken home by students. This is the only way in which we can ensure that the devices are filtered in the current environment. Michelle is working closely with the WNYRIC team in regards to enterprise solutions regarding:

- Content filtering solutions (client based or VPN route through school district WAN)
- Enterprise management of the devices wifi and/or cell access.
- WebNetwork by Stoneware to access student and staff to the necessary educational resources with authentication.

### **Vision:**

The WNYRIC continues to work with Verizon and other tablet and smartphone vendors on mobile content filtering clients, VPN mobile clients to utilize vendor filtering solutions, robust wifi solutions, and policy management. We have confirmed that the access to the IOS and Android APIs are not available

to more than 12 enterprise solution vendors. The earliest that software solutions will be available is June 2011.

The **Managed Diversity Model** is suggested in this environment as a homogeneous environment in which everyone has the same device is difficult if not impossible to achieve and maintain in this market.

We have created a survey for technology coordinators, superintendents and business officials about the tasks achieved using these devices, and how important these tasks are. This will allow us to provide a managed diversity matrix to best manage enterprise security in a cost efficient manner. Below are the components of managed scenarios.

- IT controlled - Establish a platform support level that permits a narrow set or single choice of hardware when enhanced application support is required. If you want IT to be responsible for the device – then IT has to dictate what is purchased.
- Shared IT responsibility – Establish an appliance support level for a broader set of hardware choices when applications can be constrained to support solely voice, email, personal information management and selected applications that run consistently.
- Concierge – move to individual purchases (individual liable devices) or additional hands on custom support costs for a fee.
- Combine all three to form a managed diversity matrix for up to 7 groups. Break up the user community into groups with similar needs, and then provide each user in a given group with a portfolio of devices, applications, services and privileges identical to the group – this is not cost effective as user circumvents policies leaving IT department to support personally owned machines.